Electronic Medical Records and Risk Management in Hospitals of Saudi Arabia

Abdullah Al-Barnawi, Ying He*, Leandros A.Maglaras and Helge Janicke

School of Computer Science and Informatics, De Montfort University, UK

Corresponding author: ying.he@dmu.ac.uk (Ying He)

Electronic Medical Records and Risk Management in Hospitals of Saudi Arabia

Electronic Medical Records (EMR) systems and the associated risks have been well studied in developed countries; the same cannot be said for systems in developing countries. Previous research in Saudi Arabia healthcare organisations has shown a low level of quality in hospital services due to ineffective risk management. The objective of this research is to apply the Systems Theoretic Accident Modelling and Processes (STAMP) risk management technique in Saudi Arabia and evaluate its implementation. A two- phase case study in a healthcare organisation in Saudi Arabia was conducted. The first phase implemented the STAMP technique to identify and manage risks to the system. For the second phase the STAMP technique was extended to include a Checklist, to increase STAMP's capability to mitigate risks, and the process reapplied. The results demonstrated that the inclusion of the STAMP Checklist (STAMPC) reduced errors and prevented system failures compared to regular STAMP.

Keywords: Electronic medical records (EMR); Risk management (RM); Saudi Arabia (SA); STAMP Checklist (STAMPC)

1. Introduction

In recent years, medical systems have undergone transformative changes. The integration of electronic medical records (EMR), picture archiving and communication systems (PACS), electronic prescribing (ePrescribing), associated computerised provider (or physician) order entry systems (CPOE), and computerised decision support systems (CDSSs) has increased the organisational complexity [1]. This situation requires increased risk management capacity in the healthcare system in order to improve their ability to provide safe, quality care to patients and families, and to protect hospital performance against systems failures [2].

Risk management is a demanding and challenging aspect of government electronic programmes across many sectors. Risk management is recognised as essential to the success of business, healthcare and project management, as it can save time,

reduce costs and eliminate potential failures before damage occurs [3]. There has been extensive research carried out on the benefits of risk management. It identifies favourable alternative courses of action, increases confidence in achieving project objectives, enhances chances of success as well as reduces doubts and duplication of efforts [4]. An effective risk management programme in health sectors, or elsewhere, allows better understanding of the risk involved in any initiative and allows more informed decisions to be made [5]. In healthcare, the increasing number and severity of medical errors attributable to interactions with medical equipment have led healthcare providers to recognise the importance of risk management. EMR systems have been widely adopted in developed countries with the associated risks well studied [6-10]. However, there have been fewer studies on risk management in developing countries, although some work has been done [11].

A number of techniques have been developed to analyse system incidents and failures, such as Brainstorming [12], Root Cause Analysis (RCA) [13], Failure Mode and Effects Analysis (FMEA) [14], Fault Tree Analysis (FTA) [15, 16], Binary Decision Diagrams (BDD) [17], Goal Structuring Notations (GSN) [18, 19], Generic Security Templates (GST) [20, 21] and Systems Theoretic Accident Modelling and Processes (STAMP) [22, 23]. In this research, STAMP is applied to conduct risk management of EMR systems. The technique has been applied to analyse many safety related cases and accidents [22], across sectors such as rail transport [24], water [25] and oil production [26] and is used by many organisations, such as the National Aeronautics and Space Administration (NASA). STAMP has been chosen for the following reasons: 1) it focuses on unsafe conditions or actions; 2) it incorporates the notion that a safety accident might include external disturbances; and 3) it includes both developing and operational structures [27].

The objectives of this paper were to (1) implement the STAMP technique to manage risks in a hospital in the KKGH Riyadh Region and evaluate if STAMP can reduce the failure rate in the hospital; (2) adapt and enhance the STAMP technique to mitigate risks; and (3) implement the enhanced STAMP in the same hospital in the KKGH Riyadh Region and evaluate whether the enhanced version can reduce the failure rate in the hospital. This article makes the following contributions,

- Implements and evaluates of the STAMP risk management technique in a hospital in the KKGH Riyadh Region.
- Enhances STAMP by adding a Checklist component to support and strengthen the capability to mitigate risks.
- Quantifies the improvement of STAMPC over STAMP.

The remainder of this paper is structured as follows: section 2 presents related work; section 3 discusses the methodologies; section 4 implements STAMP, whilst section 5 introduces, evaluates and compares our improved technique, STAMPC; and section 6 summarises this paper.

2. Related work

2.1. EMR Adoption

EMR systems have seen an increase in use by a number of countries. In the United States of America (USA), EMR systems have been used since the late 1960s [28]. Systems were used for processing patient information from admission through to discharge. In 2009, the president of the United States stated "To lower healthcare cost, cut medical errors, and improve care, we'll computerize the nation's health records in five years, saving billions of dollars in healthcare costs and countless lives". In total the

US government has spent $36 billion on computerising the Medicare and Medicaid projects using certified EMR, and it was estimated that 90% of the physicians and 70% of the hospitals would become “meaningful users” in ten years’ time [29]. A recent report provided by the Office of National Coordinator for Health Information Technology tracked the adoption of EMR from 2008 to 2015 [30]. The results showed that 96% of hospitals were using certified EMR technology by 2015. Adoption rates of EMR in small, rural hospitals continued to lag behind [31], although they have been steadily increasing in recent years [30].

Another example of the effective usage of EMR systems is Taiwan. The Bureau of National Health Insurance (BNHI), owned by the government, was aware of the importance of the new technology in the health arena with Taiwan’s Association for Medical informatics research group developing an EMR system structure [32]. In 2004, the BNHI distributed smart cards to every individual with the aim of reducing fraud and improving healthcare quality. In addition to tracking medical information, these smart cards stored a lot of useful healthcare information, including prescriptions, medical procedures, drug allergy history, vaccination records and information about organ donation [33]. The implementation of the EMR system in Taiwan has helped healthcare professionals enhance patient care and clinical services [34].

Oman has also deployed an integrated EMR, designed to replace paper-based manual medical records system in health institutions. The Ministry of Health (MOH) introduced the project in 1990. The deployment started in primary healthcare centres and then rolled out to hospitals. Oman’s EMR system covers registration, nursing records, physician entries, billing and nursing work reporting [11]. Moreover, it offers support in medical decision making, encourages the use of guidelines, and enhances coordination between different healthcare providers [35]. The World Health

Organisation (WHO) categorised Oman's healthcare system in 2000 as the most well organised system in the world in terms of outcomes. However, despite the system having been up and running since 1996 there are areas requiring improvement, such as confidentiality and quality of outcomes [11].

In the Kingdom of Saudi Arabia (KSA), the MOH was established in 1950 and its main objectives were to establish hospitals, dispensaries and other curative facilities. 60% of the medical services are provided by the MOH, while the rest of the services are provided by government bodies and other private service providers [36]. EMR has been used for decades in KSA. It provides benefits to physicians, ancillary departments, patients and management of almost all levels [37]. Saudi medical service providers have been increasingly relying on EMR [36, 37]. KSA lacks an integrated national network for medical records, due to the use of independent EMRs by different medical service providers. This has resulted in a number of both technical and human challenges. These include, but are not limited to economic, technical, organisational, legal, regulatory, and behavioural barriers [36, 37, 38]. Fortunately, a coordinated effort is in place to tackle those challenges and barriers, such as the establishment of the Saudi Association for Health Informatics [36].

2.2. Security Risk Management Techniques

Security Risk Management has been well studied from both technical and social perspectives [39, 40, 41].

Effective risk management activities require a systematic approach to evaluate and control the entire process. Risk management can be summarised into five steps: risk identification, risk analysis, risk assessment, risk planning and monitoring [42, 43]. Understanding the causes of system incidents and failures is important for safety and quality programmes in hospitals, as well as other organisations. A number of techniques

have been developed to achieve this. Brainstorming [12] is a traditional technique used for generating creative ideas through sharing allowing the identification of potential causes of problems and risks. RCA is an investigative procedure using a 'total system' approach, aimed at exploring the root causes of failures [13]. FMEA is a proactive risk assessment technique [14] employing a structured approach for forecasting and identifying the consequences of system failures [44] to identify the possible effects of individual failures within a system [45]. FTA was developed in the 1960s by Bell Telephone Laboratories and was used effectively in missile safety control systems [15, 16]. The BDD technique was introduced by Bryant and subsequently developed by Rauzy, to address the weaknesses of the conventional FTA approach [46].

Most of the RM techniques have been developed based on the belief that the most common reasons for accidents or event occurrence involve the failure of humans, equipment or environments to act or behave as expected [47]. However, few techniques have addressed the processes of interactions between human and machines [48]. STAMP, developed by Leveson, is based on a constraint-based model, focussing on the interaction between system components [23], characterising all risks to humans, organisations and equipment. It considers not only traditional physical failures but also dysfunctional interactions between non-failing components, errors in human decision making, diversified organisational contexts as well as unwanted situations due to inadequate enforcement of system constrains [23]. The technique has been helpful in assessing, analysing and preventing past and future accidents in electronic systems. This paper explains how STAMP could be adapted to meet the needs of a healthcare organisation in Saudi Arabia.

3. Methodology

A longitude case study was performed for this research, utilising a combination of

quantitative and qualitative research methods for data collection and analysis. The study lasted for six months and was carried in two phases in order to implement, revise and evaluate STAMP. This method allowed researchers to maintain a holistic overview of a 'real life' implementation over a period of time.

The first phase of the case study, documented in Section 4, implemented STAMP within the organisation. A real world incident is used to explain how to implement STAMP. The failure rate over two months was observed to identify any reduction during the implementation of STAMP. The second phase, documented in Section 5, revised STAMP by adding a checklist. This checklist was used to address deficiencies identified within the first phase. A further observation lasting two months was then performed to identify any improvements attributable to the implementation of the STAMP Checklist (STAMPC). As a follow up, the study continued for another two consecutive months during which the hospital continued using STAMPC. Finally, failure rates pre- and post- STAMPC implementation were considered.

In addition to the above-mentioned measurement, 224 checklists from 28 departments were collated during the second phase. Analysis of the correlation between different components within the checklist provided further understanding of interactions between different procedures.

To ensure that the investigation took place in an ethical manner consent letters were attached with the above-mentioned case study, clearly stating that participation in the study was voluntary, and that there was no penalty associated with subjects declining to participate. The Ethics Committee of the University has approved this study. The next few sections introduce this case study in detail.

4. Case Study - Phase 1

The objective of this phase was to explore the implementation of a risk management technique, STAMP, in a hospital and demonstrate the validity of this technique for EMR system failure prevention.

4.1. Implementation of STAMP

In STAMP, accidents are conceived as resulting not from component failures, but rather, from inadequate control or enforcement of safety-related constraints on the design, development, and operation of the system. STAMP is constructed from three basic concepts: constraints, hierarchical levels of control, and process models. These concepts, in turn, lead to a classification of control flaws that can lead to accidents.

Leveson's STAMP-based accident analysis introduces to the following steps, (1) construct the hierarchical conceptual structure and identify the constraints (Section 4.2); (2) identify the causes involved in the failure (Section 4.3). This should start from the technical process and use the general application knowledge to identify ineffective interaction issues involved in any failure; and (3) determine the adequacy of the constrains imposed. In most of the cases, the constraints were not identified or inadequately enforced along with other associated deficiencies of human decision-making and behaviour issues (Section 4.4 and 4.5).

4.2. The hierarchical conceptual structure

The current conceptual hierarchical control structure for ensuring safe operation of an EMR system in a hospital in Saudi is detailed below. This conceptual hierarchical structure consists of five levels: 1) the MOH, which provides rules (recognised as primary rules), budgets and standards; 2) the Directorate of Health Affairs (DOHA); 3) the Hospital Manager; 4) the IT Unit; and 5) the End Users (or human indicator), the

Administration and the Process (automated loop control). The policies are established by the top level (MOH) and are communicated to the lower levels. This approach is useful for finding, describing and analysing the reasons for lack of communication between different levels.

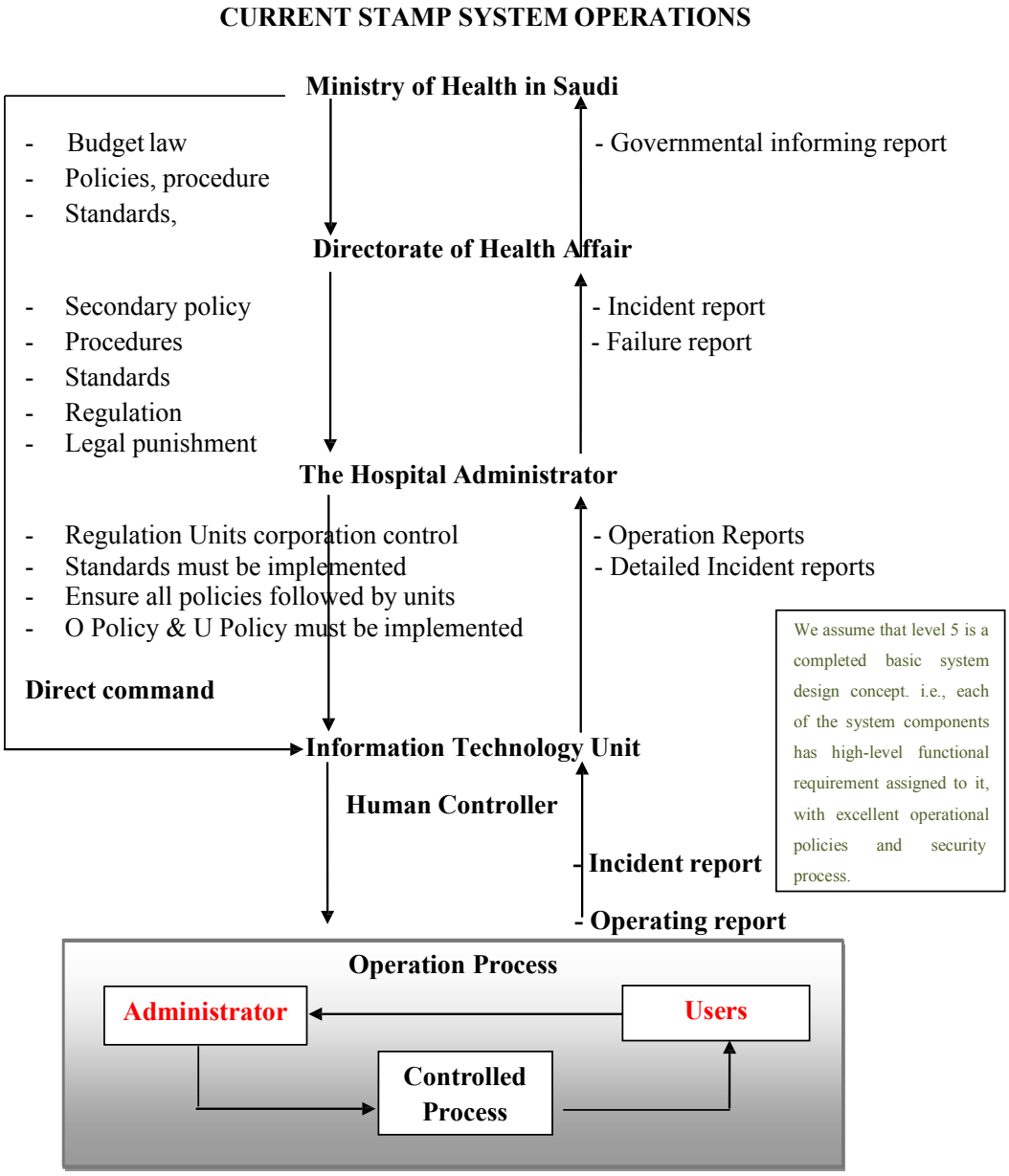

Figure 1. Classification of control flaw leading to failure check [23, 49]

Figure 1 depicts a hierarchical conceptual structure, where each stage imposes constraints on the activities of the stage below. We applied STAMP to ensure the safe operation of the EMR system, quality of service in hospitals and to identify risks leading to system failure. Downward communication channels provide the information necessary to impose behavioural constraints on the stage below; upward feedback channels provide information about how successfully these constraints have been imposed, as well as information about reported incidents.

The MOH provides budgets, laws and standards as well as policies and procedures for the Directorates of Health Affairs (DOHA). These, in addition to any guidelines, must be imposed on Hospital Managers who must ensure the implementation of these elements in all departments within the hospital.

The lower levels in this conceptual control structure include the IT administrator and systems end users, who are responsible for providing all types of reports, in addition to having direct control of the entire automated system. The IT unit is responsible for operating the system and providing safe operation requirements. End users are responsible for using the workstations and equipment correctly, in accordance with the training provided by the IT department. They must also convey information about incidents to the IT administrator or to the corresponding hospital manager and cooperate during the addressing of these incidents.

The hospital manager is responsible for establishing, implementing and controlling regulations, rules and guidelines to be followed in the hospital. In addition to making sure that the standards are effectively implemented, the hospital manager must report any uncontrollable accidents to the DOHA, who subsequently must report about accidents to the MOH. The MOH is also responsible for making changes to the policies, standards and regulations and then communicating these changes to the DOHA. In some

special cases, the MOH sends direct commands to IT Administrators. Following this model clear layers of responsibility, procedures and tasks have been defined. STAMP allows the identification of any breakdown in the model and processes outlined above.

Hospitals demand resources, such as funding, high quality medical equipment, rules, procedures, standards, effective managers and well-trained staff to manage their day-to-day activities. In many cases, rules are provided by governmental bodies, stakeholders and others. In our case, all rules are provided by the upper level or stage and imposed on the stages below.

4.2.1 Organisation of the Case Study

King Khalid General Hospital (KKGH) is located in the city of Riyadh. KKGH serves more than 650,000 people and has a capacity of 400 beds. It has been designated as a referral hospital for six other general hospitals and 20 Primary Health Care Centres (PHCCs) in the area. Until recently, not all of the facilities were electronically connected, and communication between the hospitals and the PHCCs is still performed manually. In January 2007 the MOH decided to computerise 30 hospitals throughout the kingdom of Saudi Arabia, with KKGH one of those chosen for the scheme. KKGH started using an EMR system in 2009 in almost all of its 28 clinical units (for example, in its emergency, outpatient, in-patient, radiology, laboratory, pharmacy and medical record departments). EMR was also utilised in non-clinical units, such as the patient registration, administration and discharge units. Implementation and operation of the EMR was conducted following the formal hierarchical structure, as described above (MOH, DOHA, Hospital Manager, IT Unit and IT provider),

4.2.2 The Failure at KKGH

At 6:30 am on the 26 October 2010 the EMR system suddenly failed. End users

informed the IT department immediately by telephone and requested that the system be restored. Night duty technicians reported the incident verbally to staff starting at 7:30 am, with action immediately initiated to restore the system. At approximately 7:40 am, the IT Administrator sent a request form to the provider asking for more qualified technicians to allow the determination of the root cause and identify the associated risk factors regarding the failure. As a result, actions to restore the system were delayed for approximately two hours. Additional factors contributed to the delay, including the lack of experienced computer technicians in the unit, pointing to serious problems in human resources management. The system was finally operational again approximately three hours after the incident had been reported. Fortunately, there was no serious impact on patients; however, serious attention needed to be given to investigating the failure, its causes, and the ineffective response to the situation.

The cause(s) of the failure proved difficult to determine, as KKGH did not have a properly documented incident reporting system. Also, no RM techniques were used to identify risks and prevent failures. The initial cause of the system failure was attributed to damage to some part of the server, which resulted in its breakdown. Technicians changed the damaged parts and restored the system with the help of an IT equipment provider. Fortunately, according to the IT departments report, no data were lost thanks to the backup systems in place.

According to hospitals' records, no investigation into the root causes for this system failure took place. However, many division heads did not accept that damaged components were the only cause for the failure; they questioned why the system was failing almost every week. The likelihood of this being the only cause of failure is questionable. There were potentially many other factors involved in the failure, which were beyond the control of the IT department or end users. Therefore, we used the

STAMP technique to identify the external and internal root causes of the system failure, mitigate or control current risks and prevent future failures of the EMR system.

4.3. Causal Investigation

Causal analysis starts from the technical process and uses general application knowledge to identify any ineffective interactions and communication issues involved in the failures. Based upon the investigation of this case, system risks relating to the failure were identified as follows: patients service delays; secondly, there was a lack of information exchange between care providers; and complications could occur as a result of late medical action. The system should not be turned off during busy working times should only be run by trained users. In addition, the users should understand policies, procedures and guidelines and report incidents immediately.

By using the STAMP technique, it was determined that the failure was not solely due to technical errors. Other factors also contributed to the system failure, such as the lack of periodic and timely maintenance. No documented maintenance schedule for the hardware or infrastructure appears to exist. Moreover, because end users did not systematically report incidents, upper levels were not receiving feedback on what was happening. Mistakes occurred at all levels of the hierarchy leading to the following suggested policies and constraints that the MOH should mandate in all hospitals across KSA.

4.4. Adequate policies mandated by MOH (identified using STAMP)

Well-developed policies are the fundamental requirements for the hospital to ensure the healthcare and related activities are performed safely and effectively. This subsection discusses existing MOH policies for EMR systems and RM. We present the existing MOH rules imposed on the lower levels of the hospital hierarchy, which are at the core

of its day-to-day operations. We have identified the rules that were not followed (-) and followed (+) at the hospital,

- (+) IT providers must train all users about the use of the system and its safety;
- (+) IT providers are responsible for fixing any defects in the system, for the entire period of the contract;
- (-) The operation and maintenance contract must be renewed every three years before the end of the previous agreement;
- (-) A supervisory and feedback loop must be provided to ensure that each healthcare provider's manager is doing his job adequately;
- (+) An electronic medical record must be generated for every patient of the hospital;
- (-) The periodic maintenance report must be sent from the lower levels (IT department) to the higher levels;
- (+) Any additional system enhancement requests, issued by key hospital personnel, should be developed and implemented by IT providers;
- (-) Feedback about the system operation and its faults must be reported to the higher levels in the organisational hierarchy;
- (-) Risks must be identified and treated;
- (+) Correct modification or enhancement of the EMR is required.

4.5. Inadequate Policies Enforced by the MOH and IT Unit (Identified using STAMP)

By using the STAMP technique, we found that the MOH policies lack information about the security management, risk assessment and incident response in the hospital. These included,

- Inadequate incident reporting to the hospital manager from both the IT department and end users;
- Inadequate constraints imposed by the IT manager on the users;
- Inadequate periodic maintenance of both hardware and software;
- Lack of feedback between the IT department and other department at different hierarchy levels;
- Improper identification and management of risks.

In this investigation we determined the most likely causes of the EMR system failure at KKGH: incomplete risk identification process; inadequate periodic maintenance; lack of effective feedback from managers to the lower levels; lack of effective policies; and inability to identify serious potential risks. The responsibility for a system failure generally lies within the top-level manager of hospital, who in this case did not pay much attention to risk management and failure prevention processes.

4.6. Failure Rates and Reasons for Enhancing the STAMP

The term of failure is defined as the system's inability to meet a specific stakeholder and user's expectation [50, 51]. This hospital defines failure as inability of the system to fulfil its duties, which negatively impacted the organisation's medical services. The failure rate was measured by the frequency of failures per week. Through observation, we found that the use of the original STAMP technique did not reduce the (weekly) system failure rate, and it was inadequate with respect to imposing constraints to prevent incidents. Periodic maintenance was not conducted either. This finding was not a surprise as the goals of the original STAMP technique were "to assist and understand why incidents occur " [23]. It does not have the capability to manage and mitigate risks, thereby preventing potential failures caused by the deficiencies identified in previous sections.

We therefore identified the necessity to improve the current STAMP technique in a way that it can address the deficiencies by improving the completeness and consistency of incident reports, ensuring steady process improvement, enhancing and encouraging users and the unit's directors for reporting incidents, reducing complications and prompting the appropriate management at each level. Section 5 introducs the revised STAMP and its implementation in the same organisation.

5. Case Study – Phase 2

5.1. Enhancing the STAMP Technique with a Checklist

Our idea to enhance the STAMP technique was prompted by our findings in Case Study Phase 1. We decided to add a checklist to address those deficiencies. Existing work shows that many high-technology industries, such as aviation and manufacturing quality control, rely heavily on checklists to help reduce human and technical errors. For example, Ziewacz et al. [52] stated that checklists are the standards in managing aviation and other high-reliability industry emergencies: their use helps to prioritise and standardise actions [53]. However, checklists have not achieved widespread use for healthcare failures [52].

Hales and Pronovost summarised the benefits of using checklists. The checklists can provide guidance to users, verify a task to ensure failures are avoided, and provide a framework to evaluate a process. In addition, they help to ensure adherence to 'best practice' [54]. Hundreds of organisations, including the American College of Physicians and Surgeons (ACP&S) and the America n Society of Anaesthesiologists (ASA), have supported the use of checklists for reducing errors, morbidity and mortality [55, 56]. Thus, we modified the STAMP technique by including a checklist, while ensuring that this amendment was incorporated without affecting or interfering with the design

methods of the original technique.

5.2. Development of the STAMPC Risk Management Technique

The STAMPC development was based on a literature search and the findings of the Case Study Phase 1. The initial draft of the technique was documented and circulated for expert review in the Software Technology Research Laboratory (STRL) at De Montfort University (DMU). A few modifications were made to the first draft. The added checklist had 15 questions (Appendix A). The checklist was also presented to an audience at the Saudi Scientific International Conference in the UK for further feedback.

Figure 2 illustrates the main features of the STAMP Checklist (STAMPC). Similar to Figure 1, the structure takes into account the EMR's system operations and shows the communication between different hierarchical levels. We included the checklist component named "RM STAMP Checklist", which can capture incident and operating items. We also added a feedback mechanism named "Paper feedback" and incident report processes associated with the checklist. The STAMPC was implemented with support from the IT, quality improvement and EMR Unit Managers along with other users at KKGH in Al-Khar

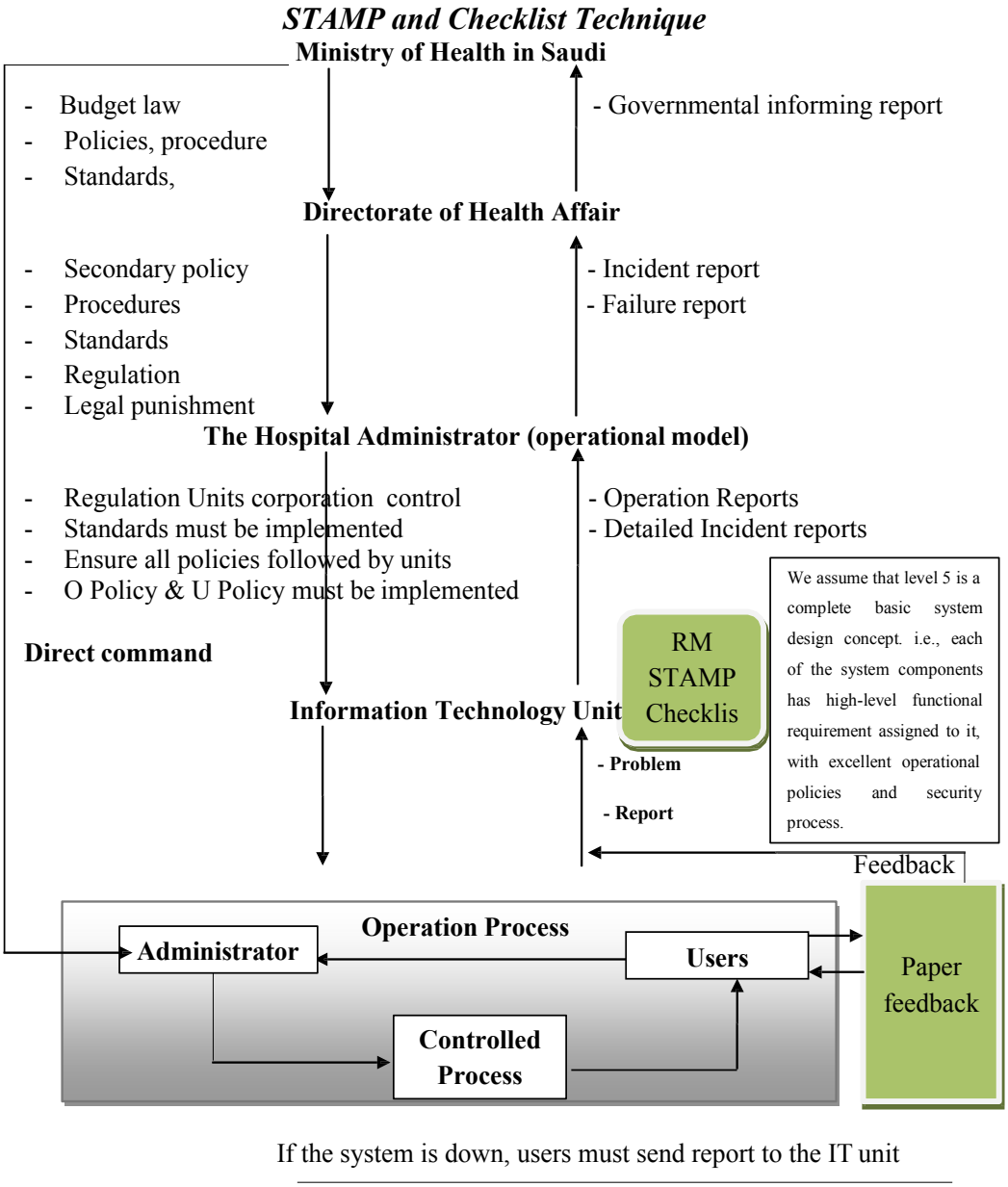

Figure 2. Classification of control flaws leading to failure (STAMP Checklist based on STAMP); an analysis of EMR systems using the STAMPC technique.

5.3. The STAMPC Technique and its Practical Application for EMR

The STAMPC passed through accreditation of the Central Board for Accreditation of Healthcare (CBAHI). The quality management programme, EMR system and safety policies and standards were effectively endorsed, implemented and communicated to

users and staff across the hospital. The implementation of STAMPC was relatively straightforward. The trial was conducted over a period of two months.

The steps of this trial were as follows: 1) we organised a meeting with the unit heads, who volunteered to participate in the study and provide feedback on the contents; 2) we gave a presentation about the value of the STAMPC technique for managing risks and preventing failures; and 3) we made sure that the policies, standards and the incident reporting forms were in place that end users were aware of them and that the EMR system provider was informed about the importance of periodic maintenance. A formal schedule was proposed and agreed upon; the hospital director agreed to verify and follow up on the application of the added checklist.

Before the formal launch of the use of the checklist, we gave a short presentation that described the background of the technique and provided some basic guidelines for using the checklist. Nearly all EMR system users in the hospital received this overview. The Quality and Safety Committee team members of the hospital were asked to volunteer for a series of tasks, including assisting us in distributing and collecting the completed checklists weekly and to make sure that the IT department reported feedback. Once the checklist and the implementation process had been introduced and mandated in all departments, a copy of the checklist was sent to each department. We requested the checklist to be filled in and returned to us for analysis. The units were given the option to store the forms in a box on site, which was also available to us. We closely monitored each unit to ensure that the checklist and the incident reports were used when necessary. In addition, feedback was requested from the IT department after the task was completed. The lead researcher took care to ensure that every participant was comfortable with his or her role and actions and provided feedback to them.

5.4. STAMPC evaluation results

This subsection reports our findings from the application of the STAMPC technique at KKGH. A total of 224 checklists were completed over the 2-month period (112 for each month). Our sampling included all departments in the hospital that were using the EMR system. A total of 28 departments were included in the survey: 27 clinical and one nonclinical (the Admission and Discharge Unit). Before using the STAMP Checklist, we predicted that system maintenance would decrease the rate of system failures and maximise the quality of the hospital's performance. All completed checklists were collected and analysed using Pearson correlation in SPSS in order to identify the relationship between different variables (i.e. questions in the checklist).

Outcomes of the analysis conducted using the Pearson correlation coefficient are shown in Table 1. We coded the answers for all 15 questions, using 1 for "Yes" -1 for "No" and 0 for "I do not know". This coding was suitable for most questions except for Question 11, for which, we coded "1" for maintenance performed every 6 months, "0" for maintenance performed every 12 months and "-1" for "maintenance never done". The correlation table shows that there is significant correlation between the answers for Questions 1, 2, and 3. In addition, there is a weak negative correlation between the answers for Questions 11 and 12, which implies that any increase in the frequency of maintenance will lead to a decrease in the failure rate.

Table 1. Correlation between the variables

		Q1	Q2	Q3	Q11	Q12
Q1	Pearson Correlation	1	.454**	.521**	.504**	.021
	Sig. (2-tailed)		.000	.000	.000	.750
Q2	Pearson Correlation	.454**	1	1.521**	.377**	.036
	Sig. (2-tailed)	.000		.000	.000	.592
Q3	Pearson Correlation	.521**	.551**	1	.472**	.082
	Sig. (2-tailed)	.000	.000		.000	.222
Q11	Pearson Correlation	.504**	.377**	.472**	1	-.073
	Sig. (2-tailed)	.000	.000	.000		.276
Q12	Pearson Correlation	.021	.036	.082	-.073	1
	Sig. (2-tailed)	.750	.592	.222	.276	

5.5. Failure Rates Analysis and Comparisons

Through observation, we found that during the time that the checklist was applied, the EMR system failure rate fell considerably to only one per month. This is considered to be a significant achievement. The IT department performed its job perfectly; in particular, periodic maintenance for both hardware (HW) and software (SW) was performed on time and according to the plan. Users have started to use the formal incident reporting form regularly and all users have received immediate feedback after actions were taken. Recall our findings in Section 4. The use of the original STAMP technique failed to reduce the (weekly) system failure rate, and it was inadequate with respect to imposing constraints to prevent incidents. Existing work has shown that the use of checklists can improve safety and help to manage system failures [52]. One characteristic of the STAMPC technique is that it includes an explicit operational definition of its process and is therefore perceived as a systematic risk management process compared to the regular STAMP technique. Our findings showed that the checklist could detect additional information to prevent failures and reduce the number of risk factors that led to failures. The study continued for another two consecutive months.

For the two consequent months, the hospital's units continued using the checklist every week as planned by the researcher during the study. The quality management team reported that the EMR system failure in the hospital reduced to nil for two months. We expected that the EMR systems failure would be reduced to the lowest rate (less than once a year) if the application of the STAMPC continued as planned. This finding showed the benefits of applying a checklist with STAMP. The data extracted using STAMPC, provided users and managers with useful information to

prevent failures and to improve safety in the context of a hospital that has identifiable issues with their ERM system.

6. Discussion

Previous studies in Saudi Arabia showed that their EMR were still not mature due to the lack of periodic maintenance and management. Traditional brainstorming risk management techniques were used in some hospitals to detect risks and prevent failures [57]. However, no systematic risk management technique had been applied in hospital in Saudi Arabia before.

This study consists of two phases. During the first phase we applied the STAMP technique to identify risks of the EMR systems, and possible causes of failures. The main findings from this phase were, inadequate incident reporting to the hospital manager from the IT department and end users, inadequate constraints imposed by the IT manager on end users, inadequate periodic maintenance of hardware/software and other infrastructure, lack of feedback between IT department and other levels in the hierarchy and poor identification as well as management of risks.

During the second phase, our proposed method, namely STAMPC, was used for a period of two months. Main objective of this stage was to identify further causal factors in addition to the findings of the first phase in order to mitigate risks and reduce weekly EMR failures. The main outcome of the application of STAMPC was the reduction of the EMR failure rate from once every week to nearly once every month. Compared to the STAMP technique, STAMPC technique has been provided to be more affective. Data extracted using STAMPC were found to be useful for both stakeholders and users for improving safety and preventing potential system failures. Moreover, the STAMPC technique ensures that all interactions between different organisational levels, throughout the EMR system life cycle, are taken into account. STAMPC facilitates the

identification, development and implementation of strategies and procedures that are necessary to identify and avoid potential risks [58, 59].

7. Conclusions and future work

This study sets out to tackle two important problems, namely, continuous system failures and the lack of risk management technique usage in hospitals in Saudi Arabia. Previous research in the Saudi Arabia healthcare organisations showed that there was a low level of quality in hospital services, which was due to the lack of effective risk management policies, risk assessment procedures and project management [57]. This research applied the STAMP technique to detect risks and analysed system failures of KKG hospitals that use EMR system. Specifically, the technique was used to help system stakeholders, including providers and end users, consider the system through its entire life cycle and take into account all interactions between different levels in the hierarchy. The obvious advantage of STAMP technique was that it provided an opportunity (and reason) to create an overall view of the entire system dealing with interactions between humans, the organisations and technologies. The use of STAMP guided users to identify the causal factors of incidents. STAMP technique made it possible to identify potential risks by providing detailed scenarios involving incident components.

The application of the STAMP technique with the addition of a checklist, the STAMPC technique, in a real hospital environment, significantly improved the quality of the hospital's performance and reduced systems' failure rate. The incorporation of the checklist with the STAMP technique has been proven to be useful. By using this tool, the root causes of failures were identified, allowing the hospital to avoid potential system failures and other adverse incidents. This case study has provided the first testing of the use of the risk assessment technique STAMP in an EMR system in the

KSA and has made a significant contribution in reducing the failure rate of the local hospital, KKGH. The study also contributed to the knowledge by broadening the scope of literature on EMR systems and effective RM in hospitals in Saudi Arabia and elsewhere, in particular, by proposing a new method, namely STAMPC, to identify and mitigate system failures. Further studies should encompass wider and different geographical healthcare providers, including both public and private sectors. Future work will also include the adaption of the STAMPC to meet specific needs of other hospitals or organisations.

Appendix A.

Table A1. STAMP Checklist for RM in EMR Systems

No.	Review Required	Yes	No	I don't know
1	Have you received updated EMR policies and procedure from MOH or the Information Technology unit recently?			
2	Do the policies involve instruction for contacting IT expert 24-hours a day?			
3	Are you aware of the policies, procedures and standards of this hospital?			
4	Have all users been trained, on the hospital and the IT security policies and procedure?			
5	Do only authorised staffs have access to the system?			
6	Do all users have passwords and usernames?			
7	Do you know whom to contact in case of incident?			
8	Is your computer protected by virus protection software?			
9	Does your computer receive virus protection updates?			
10	Has the IT technicians performed system software maintenance this week?			
11	When was the last hardware precaution maintenance done?	6M	12M	Never Heard
12	Have you filled in any incident report this week?			
13	Have you received feedback for previous incident report?			
14	If the IT technician dose not respond, does a procedure exist for escalating the problem to the hospital manager?			
15	Do incident-report form and procedures exist?			

References

[1] A. D. Black, J. Car, C. Pagliari, C. Anandan, K. Cresswell, T. Bokun, B. McKinstry, R. Procter, A. Majeed, A. Sheikh, et al., The impact of ehealth on the quality and safety of health care: a systematic overview, PLoS medicine 8 (1) (2011) 188.

[2] A. C. Cagliano, S. Grimaldi, C. Rafele, A systemic methodology for risk management in healthcare sector, Safety Science 49 (5) (2011) 695–708.

[3] D. Hillson, R. Murray-Webster, Understanding and managing risk attitude, Gower Publishing, Ltd., 2007.

[4] P. L. Bannerman, Risk and risk management in software projects: A reassessment, Journal of Systems and Software 81 (12) (2008) 2118–2133.

[5] A. Holmes, Smart risk, John Wiley & Sons, 2004.

[6] A. Sunyaev, J. Pflug, Risk evaluation and security analysis of the clinical area within the german electronic health information system, Health and Technology 2 (2) (2012) 123–135.

[7] D. W. Bates, R. S. Evans, H. Murff, P. D. Stetson, L. Pizziferri, G. Hripcsak, Detecting adverse events using information technology, Journal of the American Medical Informatics Association 10 (2) (2003) 115–128.

[8] C. Vincent, G. Neale, M. Woloshynowych, Adverse events in british hospitals: preliminary retrospective record review, Bmj 322 (7285) (2001) 517–519.

[9] F. Le Duff, S. Daniel, B. Kamendj´e, P. Le Beux, R. Duvauferrier, Monitoring inci- dent report in the healthcare process to improve quality in hospitals, International journal of medical informatics 74 (2) (2005) 111–117.

[10] J. P. Daniels, A. D. King, D. D. Cochrane, R. Carr, N. T. Shaw, J. Lim, J. M. Ansermino, A human factors and survey methodology-based design of a web-based adverse event reporting system for families, International journal of medical infor- matics 79 (5) (2010) 339–348.

[11] S. Ajami, T. Bagheri-Tadi, Barriers for adopting electronic health records (ehrs) by physicians, Acta Informatica Medica 21 (2) (2013) 129.

[12] C. H. Clark, Brainstorming: The dynamic new way to create successful ideas, Diamonds, 2014.

[13] A. Raghavan, Root cause analysis, in: Management and Leadership–A Guide for Clinical Professionals, Springer, 2015, pp. 105–121.

[14] D. Natarajan, Failure mode and effects analysis, in: Reliable Design of Electronic Equipment, Springer, 2015, pp. 31–44.

[15] A. Park, S. J. Lee, Fault tree analysis on hand washing for hygiene management, Food Control 20 (3) (2009) 223–229.

[16] M. Walker, Y. Papadopoulos, Synthesis and analysis of temporal fault trees with pandora: The time of priority and gates, Nonlinear Analysis: Hybrid Systems 2 (2) (2008) 368–382.

[17] R. Drechsler, B. Becker, Binary decision diagrams: theory and implementation, Springer Science & Business Media, 2013.

[18] T. Kelly, R. Weaver, The goal structuring notation–a safety argument notation, in: Proceedings of the dependable systems and networks 2004 workshop on assurance cases, Citeseer, 2004.

[19] M. A. Sujan, I. Habli, T. P. Kelly, S. Pozzi, C. W. Johnson, Should healthcare providers do safety cases? lessons from a cross-industry review of safety case prac- tices, Safety Science 84 (2016) 181–189.

[20] Y. He, C. Johnson, Y. Lyu, A. Ahmad, Improving the exchange of lessons learned in security incident reports: Case studies in the privacy of electronic patient records, in: Trust Management VIII, Springer, 2014, pp. 109–124.

[21] Y. He, C. Johnson, Improving the redistribution of the security lessons in health- care: An evaluation of the generic security template, International Journal of Med- ical Informatics 84 (11) (2015) 941–949.

[22] H. Altabbakh, M. A. AlKazimi, S. Murray, K. Grantham, Stamp–holistic system safety approach or just another risk model?, Journal of Loss Prevention in the Process Industries 32 (2014) 109–119.

[23] N. Leveson, A new accident model for engineering safer systems, Safety science 42 (4) (2004) 237–270.

[24] P. Underwood, P. Waterson, Systems thinking, the swiss cheese model and accident analysis: A comparative systemic analysis of the grayrigg train derailment using the atsb, accimap and stamp models, Accident Analysis & Prevention 68 (2014) 75–94.

[25] N. Leveson, M. Daouk, N. Dulac, K. Marais, Applying stamp in accident analysis, in: NASA Conference Publication, NASA; 1998, 2003, pp. 177–198.

[26] K. Hardy, F. Guarnieri, Modelling and hazard analysis for contaminated sediments using stamp model, in: 14th International Conference on Process Integration, Modelling and Optimisation for Energy, Saving and Pollution Reduction, Vol. 25, 2011, pp. 737–742.

[27] N. G. Leveson, Model-based analysis of socio-technical risk, Massachusetts Institute of Technology, ESD-WP-2004-08.

[28] E. H. Shortliffe, Strategic action in health information technology: why the obvious has taken so long, Health Affairs 24 (5) (2005) 1222–1233.

[29] R. Nelson, N. Staggers, Health informatics: An inter professional approach, Elsevier Health Sciences, 2013.

[30] J. Henry, Y. Pylypchuk, T. Searcy, V. Patel, Adoption of electronic health record systems among us non-federal acute care hospitals: 2008-2015, The Office of Na- tional Coordinator for Health Information Technology.

[31] J. Adler-Milstein, C. M. DesRoches, P. Kralovec, G. Foster, C. Worzala, D. Charles, T. Searcy, A. K. Jha, Electronic health record adoption in us hospitals: progress continues, but challenges persist, Health Affairs 34 (12) (2015) 2174–2180.

[32] H.-H. Rau, C.-Y. Hsu, Y.-L. Lee, W. Chen, W.-S. Jian, Developing electronic health records in taiwan, IT professional (2) (2010) 17–25.

[33] M.-H. Hsu, J.-C. Yen, W.-T. Chiu, S.-L. Tsai, C.-T. Liu, Y.-C. Li, Using health smart cards to check drug allergy history: The perspective from taiwans experi- ences, Journal of medical systems 35 (4) (2011) 555–558.

[34] Y.-Y. Su, K. T. Win, H.-C. Chiu, The development of taiwanese electronic medical record systems evaluation instrument.

[35] A. Al-Mujaini, Y. Al-Farsi, A. Al-Maniri, A. Ganesh, Satisfaction and perceived quality of an electronic medical record system in a tertiary hospital in oman, Oman medical journal 26 (5) (2011) 324.

[36] M. M. Altuwaijri, Electronic-health in saudi arabia, Saudi medical journal 29 (2) (2008) 171–178.

[37] M. Khalifa, Barriers to health information systems and electronic medical records implementation. a field study of saudi arabian hospitals, Procedia Computer Science 21 (2013) 335–342.

[38] M. Khalifa, Technical and human challenges of implementing hospital information systems in saudi arabia, Journal of Health Informatics in Developing Countries 8 (1).

[39] D. G. Manuel, K. E. Abdulaziz, R. Perez, S. Beach, C. Bennett, Personalized risk communication for personalized risk assessment: Real world assessment of knowl- edge and motivation for six mortality risk measures from an online life expectancy calculator., Informatics for health & social care (2017) 1.

[40] Y. Peng, E. Erdem, J. Shi, C. Masek, P. Woodbridge, Large-scale assessment of missed opportunity risks in a complex hospital setting, Informatics for Health and Social Care 41 (2) (2016) 112–127.

[41] M. Gissler, Assessment of environmental health risks is feasible by secondary use of administrative registers, Informatics for Health and Social Care 38 (3) (2013) 291–301.

[42] C. Lindholm, M. Host, Risk identification by physicians and developers-differences investigated in a controlled experiment, in: Proceedings of the 2009 ICSE Workshop on Software Engineering in Health Care, IEEE Computer Society, 2009, pp. 53–61.

[43] N. Sun, L. Wang, J. Zhou, Q. Yuan, Z. Zhang, Y. Li, M. Liang, L. Cheng, G. Gao, X. Cui,

International comparative analyses of healthcare risk management, Journal of Evidence-Based Medicine 4 (1) (2011) 22–31.

[44] K. T. Win, H. Phung, L. Young, M. Tran, C. Alcock, K. Hillman, Electronic health record system risk assessment: a case study from the minet, Health Information Management 33 (2) (2004) 43–48.

[45] D. Marx, A. Slonim, Assessing patient safety risk before the injury occurs: an introduction to sociotechnical probabilistic risk modelling in health care, Quality and Safety in Health Care 12 (suppl 2) (2003) ii33–ii38.

[46] A. Rauzy, New algorithms for fault trees analysis, Reliability Engineering & System Safety 40 (3) (1993) 203–211.

[47] D. E. Doytchev, G. Szwillus, Combining task analysis and fault tree analysis for accident and incident analysis: a case study from bulgaria, Accident Analysis & Prevention 41 (6) (2009) 1172–1179.

[48] T. Moriyama, H. Ohtani, Risk assessment tools incorporating human error prob- abilities in the japanese small-sized establishment, Safety science 47 (10) (2009) 1379–1397.

[49] M. Ouyang, L. Hong, M.-H. Yu, Q. Fei, Stamp-based analysis on the railway acci- dent and accident spreading: Taking the china–jiaoji railway accident for example, Safety science 48 (5) (2010) 544–555.

[50] K. Lyytinen, R. Hirschheim, Information systems failures a survey and classification of the empirical literature, in: Oxford surveys in information technology, Oxford University Press, Inc., 1988, pp. 257–309.

[51] Y. K. Dwivedi, D. Wastell, S. Laumer, H. Z. Henriksen, M. D. Myers, D. Bunker, A. Elbanna, M. Ravishankar, S. C. Srivastava, Research on information systems failures and successes: Status update and future directions, Information Systems Frontiers 17 (1) (2015) 143–157.

[52] J. E. Ziewacz, A. F. Arriaga, A. M. Bader, W. R. Berry, L. Edmondson, J. M. Wong, S. R. Lipsitz, D. L. Hepner, S. Peyre, S. Nelson, et al., Crisis checklists for the operating room: development and pilot testing, Journal of the American College of Surgeons 213 (2) (2011) 212–217.

[53] N. Burbos, E. Morris, Applying the world health organization surgical safety checklist to obstetrics and gynaecology, Obstetrics, Gynaecology & Reproductive Medicine 21 (1) (2011) 24–26.

[54] B. M. Hales, P. J. Pronovost, The checklista tool for error management and performance improvement, Journal of critical care 21 (3) (2006) 231–235.

[55] K. A. Styer, S. W. Ashley, I. Schmidt, E. M. Zive, S. Eappen, Implementing the world health organization surgical safety checklist: a model for future perioperative initiatives, AORN journal 94 (6) (2011) 590–598.

[56] P. J. Pronovost, C. A. Goeschel, J. A. Marsteller, J. B. Sexton, J. C. Pham, S. M. Berenholtz, Framework for patient safety research and improvement, Circulation 119 (2) (2009) 330–337.

[57] A. Barnawi, Risk Management of Electronic Health Record System in Hospitals, De Montfort University, 2013.

[58] S. Abdel-Rehim, A. Morritt, G. Perks, Who surgical checklist and its practical application in plastic surgery, Plastic surgery international 2011.

[59] M. Evans, L.A. Maglaras, Y. He, H. Janicke, Human behaviour as an aspect of cybersecurity assurance. Security and Communication Networks, 9(17), 4667-4679, 2016.